IN THE CLAIMS:

Please amend claims 1, 6, 10, 14, 17, 21, and 25 as follows:

1. (Currrently amended) A method of accessing a password comprising:

dividing the password received from a client into a plurality of pieces by taking a plurality of hashes of the password, each hash using a different salt value to obtain a plurality of hash values, from each of which a predetermined number of bits are taken to represent each password piece of the plurality of pieces;

storing each piece of the plurality of pieces of the password on a different one of a plurality of servers, each of the plurality of servers being independent from others of the plurality of servers;

separately authenticating a user at each of the plurality of servers, each of the plurality of servers transmitting the piece of the password stored at the respective server to the user when the authentication at that server is successful;

assembling the password from the password pieces transmitted from the plurality of servers; and

deleting the password and the plurality of pieces of the password from the client.

2. (Original) The method of claim 1, wherein the password is a private key in a public/private key pair.

3. (Original) The method of claim 1, wherein a second password is used to authenticate the user at each of the plurality of servers, the second password being a weak password.

4. (Original) The method of claim 3, wherein each of the pieces of the password are encrypted before being stored on each of the servers, encryption keys for the encryption of the password pieces being derived from the second password.

5. (Canceled)

6. (Currently Amended) A method of securely storing a password comprising:

receiving an encrypted portion of the password, the encrypted portion of the password comprising less than the entire password and being derived by taking a plurality of hashes of the password, each hash using a different salt value to obtain a plurality of hash values, from each of which a predetermined number of bits are taken to represent the portion of the password which is then encrypted;

storing the encrypted portion of the password with identification information for a user of the encrypted portion of the password;

receiving a request for the encrypted portion of the password, the request including the identification information; and

returning the encrypted portion of the password to the user when the identification information in the request matches the stored identification information.

7. (Original) The method of claim 6, wherein the password is a private key in a public/private key pair.

8. (Original) The method of claim 6, wherein the received encrypted portion of the password is encrypted based on a symmetric encryption of the portion of the password using a key based on a second password, the second password being a weak password.

9. (Previously Presented) The method of claim 8, wherein the identification information of the user of the encrypted portion of the password is based on the second password.

10. (Currently Amended) A method of receiving a first password of a user, the method comprising:

entering a second password of the user;

authenticating the user at each of a plurality of servers based on the second password, the

plurality of servers being independent from one another;

receiving an encrypted version of a portion of the first password from each of the plurality of servers at which the authentication was successful, each of the portions of the first password containing less than the entire password, and the portion of the first password being derived by taking a plurality of hashes of the first password, each hash using a different salt value to obtain a plurality of hash values, from each of which a predetermined number of bits are taken to represent the portion of the first password;

decrypting the received encrypted portions of the first password using encryption keys based on the second password; and

assembling the first password from the decrypted portions.

11. (Original) The method of claim 10, wherein the first password is a strong user password.

12. (Original) The method of claim 10, wherein the first password is a private key in a public/private key pair.

13. (Original) The method of claim 10, wherein the second password is a weak password.

14. (Currently Amended) A method of authenticating a user at a remote computer system comprising:

dividing a password entered by the user into a plurality of pieces by taking a plurality of hashes of the password, each hash using a different salt value to obtain a plurality of hash values, from each of which a predetermined number of bits are taken to represent each piece of the plurality of pieces of the password;

transmitting each piece of the plurality of pieces to corresponding ones of a plurality of remote servers, each of the plurality of remote servers being independent from others of the plurality of remote servers, and each of the remote servers having a respective piece of the

plurality of pieces of the password pre-registered with the remote server;

comparing the transmitted piece of the plurality of pieces of the password to the pre-registered piece of the password at the plurality of servers;

generating an authentication accept message at each of the plurality of servers at which the pre-registered piece of the password matches the transmitted piece of the plurality of pieces of the password; and

authenticating the user when the authentication accept message is generated for all of the plurality of pieces of the password at the plurality of servers.

15. (Original) The method of claim 14, wherein a piece of the password is pre-registered at a computer local to the user and the authentication accept message is generated by the computer local to the user when the pre-registered piece of the password at the computer local to the user matches a corresponding piece of the password entered by the user.

16. (Original) The method of claim 15, wherein the authentication accept messages are received and accepted at a content server remote from the user.

17. (Currently Amended) A computer server comprising:

a computer memory; and

a processor coupled to the computer memory, wherein

the processor ~~receiving~~ receives an encrypted portion of a password, the encrypted portion of the password comprising less than the entire password, the encrypted portion of the password being derived by taking a plurality of hashes of the password, each hash using a different salt value to obtain a plurality of hash values, from each of which a predetermined number of bits are taken to represent the portion of the password which is then encrypted[[;]] ~~storing over a secure connection~~ the encrypted portion of the password is stored with

identification information of a user of the encrypted portion of the password over a secure connection, [[;]] ~~receiving~~ a request for the encrypted portion of the password is recieved, the request including the identification information[[;]] , ~~and returning~~ the encrypted portion of the password is returned to the user when the identification information in the request matches the stored identification information[[;]] , and ~~wherein~~ the computer server is independent of other computer servers storing other portions of the password.

18. (Original) The computer server of claim 17, wherein the password is a private key in a public/private key pair.

19. (Original) The computer server of claim 17, wherein the received encrypted portion of the password is encrypted based on a symmetric encryption of the portion of the password using a key based on a second password, the second password being a weak password.

20. (Previously Presented) The computer server of claim 19, wherein the identification information of the user of the encrypted portion of the password is based on the second password.

21. (Currently Amended) A computer readable medium containing computer instructions that when executed by a processor cause the processor to perform operations for securely storing a password comprising:

receiving an encrypted portion of the password, the encrypted portion of the password comprising less than the entire password and being derived by taking a plurality of hashes of the password, each hash using a different salt value to obtain a plurality of hash values, from each of which, a predetermined number of bits are taken to represent the portion of the password which is then encrypted;

storing over a secure connection the encrypted portion of the password with identification

information of a user of the encrypted portion of the password;

receiving a request for the encrypted portion of the password, the request including the identification information; and

returning the encrypted portion of the password to the user when the identification information in the request matches the stored identification information.

22. (Original) The computer readable medium of claim 21, wherein the password is a private key in a public/private key pair.

23. (Original) The computer readable medium of claim 21, wherein the received encrypted portion of the password is encrypted based on a symmetric encryption of the portion of the password using a key based on a second password, the second password being a weak password.

24. (Previously Presented) The computer readable medium of claim 23, wherein the identification information of the user of the encrypted portion of the password is based on the second password.

25. (Currently Amended) A computer readable medium containing computer instructions that when executed by a processor cause the processor to perform operations that receive a first password of a user, comprising:

receiving a second password entered by the user;

authenticating the user at each of a plurality of servers based on the second password, the plurality of servers being independent from one another;

receiving an encrypted version of a portion of the first password from each of the plurality of servers at which the authentication was successful, each ~~of the~~ portion[[s]] of the first password containing less than the entire password and being derived by taking a plurality of hashes of the first password, each hash using a different salt value to obtain a plurality of hash

values, from each of which a predetermined number of bits are taken to represent the portion of the first password;

decrypting the received encrypted portions of the first password using encryption keys based on the second password; and

assembling the first password from the decrypted portions.

26. (Original) The computer readable medium of claim 25, wherein the first password is a strong user password.

27. (Original) The computer readable medium of claim 25, wherein the first password is a private key in a public/private key pair.

28. (Original) The computer readable medium of claim 25, wherein the second password is a weak password.

///

///

///

///

///

///

///

///

///